JAARUPDATE
IT & IT outsourcing

2021

In haar Staat van de Unie riep de voorzitter van de Europese Commissie op tot extra inspanningen om de digitale transformatie vorm te geven, want “digitale technologie maakt het verschil tussen succes en mislukking”. Een daarmee samenhangend speerpunt in het beleid van de Europese Commissie blijft cybersecurity, wat is terug te zien in de vele initiatieven op dit gebied. Ook in het nationale beleid zien we dat beide speerpunten volop de aandacht hebben. In de IT-rechtspraak is cybersecurity eveneens een thema, wat terugkomt in uitspraken over de verantwoordelijkheid voor back-ups. Wat opvalt in de IT-rechtspraak van het afgelopen jaar, is dat de zorgplicht minder dominant aanwezig was en dat bij meerdere thema’s werd teruggegrepen op uitleg van de overeenkomst. Deze en andere ontwikkelingen kunt u lezen in deze jaarupdate.

Ontwikkelingen

Europees niveau

Digitaal decennium

In maart 2021 presenteerde de Europese Commissie (ook “Commissie”) het digitaal kompas. In de mededeling zijn een visie, doelstellingen en trajecten voor een succesvolle digitale transformatie van de Europese Unie tegen 2030 gepresenteerd. Het in september 2021 gepubliceerde beleidsprogramma is bedoeld om ervoor te zorgen dat de EU haar doelstellingen en streefcijfers haalt op het gebied van de digitale transformatie van de samenleving en economie. Het Commissievoorstel wordt momenteel besproken in de Raad van Ministers (ook ‘Raad’).

In het kader van de financiering van de digitale transformatie is door het programma Digitaal Europa voor de jaren 2021-2027 7,59 miljard euro beschikbaar gesteld. Klik hier voor meer informatie, waar ook te lezen is welk soort projecten in aanmerking kunnen komen voor financiering. Digitaal Europa is opgericht om ervoor te zorgen dat onderzoeksresultaten op het gebied van digitale technologieën daadwerkelijk worden omgezet in producten die op de markt komen. Dit programma is onderdeel van de Langetermijnbegroting (MFK) van de EU.

Digital Services Act & Digital Markets Act

De Raad van Ministers heeft inmiddels een akkoord bereikt over de tekst van de Digital Services Act en de Digital Markets Act. De Digital Services Act biedt een kader van gelaagde verantwoordelijkheden voor onlinediensten zoals tussenpersonen, hosting-diensten en online platforms. Deze verduidelijkt de verantwoordelijkheden van deze partijen richting professionele afnemers en consumenten en verbetert de bestrijding van illegale inhoud. De Digital Markets Act introduceert verplichtingen voor de wereldwijd opererende tien tot vijftien grootste online platforms met een poortwachtersfunctie. Over de tekst van de verordeningen zal nu onderhandeld worden met het Europees Parlement en de Europese Commissie. Het streven is om een definitief akkoord te bereiken in 2022.

Cybersecurity

Op 22 maart 2021 heeft de Raad conclusies aangenomen over de in 2020 gepresenteerde cybersecuritystrategie. De Raad benadrukt in de conclusies dat cyberbeveiliging van essentieel belang is voor de opbouw van een veerkrachtig, groen en digitaal Europa. De Raad wijst in de conclusies op een aantal actiegebieden voor de komende jaren, zoals plannen voor een netwerk van operationele beveiligingscentra om aanvallen op net-werken te monitoren en erop te anticiperen, de oprichting van een gezamenlijke cybereenheid en de ontwikkeling van sterke versleuteling. Een actieplan zal ervoor moeten zorgen dat de conclusies ook worden uitgevoerd.

Met het voorstel voor een Digital Operational Resilience Act wil de Europese Commissie een regelgevingskader tot stand brengen om de digitale weerbaarheid van de financiële sector te vergroten en op die manier cyberdreigingen voorkomen en beperken. DORA stelt eisen aan financiële organisaties ten aanzien van IT-risicomanagement, IT-incidenten, periodieke testen van digitale weerbaarheid en de beheersing van risico’s bij uitbesteding aan (kritieke) derden. DORA zal van toepassing zijn op onder meer banken en verzekeraars, maar ook ICT-leveranciers van financiële bedrijven. De AFM verwacht dat de verordening op zijn vroegst eind 2022 in werking

treedt. Volgens het voorstel voor de verordening wordt de verordening twaalf maanden na inwerkingtreding van toepassing. Voor achtergrond-informatie klik hier.

De Raad is in december 2021 een standpunt overeengekomen inzake de vervanging van de NIS-Richtlijn (op 9 november 2018 geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen) door Richtlijn NIS2. De NIS-Richtlijn verplicht aanbieders van essentiële diensten (AED's) en digitale dienstverleners om passende en evenredige technische en organisatorische maatregelen op het gebied van cybersecurity te nemen. Ook geldt voor hen een meldplicht voor incidenten met aanzienlijke gevolgen voor hun dienstverlening. De NIS-Richtlijn werd echter door een veranderende manier van cyberdreiging en de digitale transformatie van de samenleving niet meer up-to-date geacht. De *nieuwe* Richtlijn NIS2 moet door middel van minimum-regelgeving de verschillen wegnemen tussen regels voor en aanpak van cyberbeveiliging in de verschillende lidstaten. Beveiligingsverplichtingen van bedrijven worden scherper en toezichtsmaatregelen voor nationale autoriteiten worden strenger. Daarnaast voert de voorgestelde Richtlijn NIS2 een “size cap”-regel in, terwijl de lidstaten onder de NIS-richtlijn zelf moeten bepalen welke entiteiten aan de criteria van aanbieder van essentiële diensten voldoen. Deze factsheet op de website van de Europese Commissie geeft een handig overzicht van de verschillen tussen de Richtlijnen.

Verder wordt er gewerkt aan de ontwikkeling van Europese cybersecurity-certificeringsschema’s. De verwachting is dat het cybersecurity-certificeringsschema voor beveiligingselementen van ICT-producten in de eerste helft van 2022 gereed is. Het certificeringsschema voor clouddiensten volgt dan in de tweede helft van 2022. Daarnaast wordt door het Europese agentschap voor cybersecurity (ENISA) een aanvang gemaakt met de ontwikkeling van een cybersecurity-certificeringsschema voor 5G-netwerkapparatuur. Ook zijn er inmiddels Europese cybersecurity-certificeringsschema’s voor Internet of Things-apparatuur en geautomatiseerde industriële controlesystemen aangekondigd.

In het kader van het versterken van de beveiliging van het internet en andere kritieke netwerk- en informatiesystemen, heeft de oprichting van het EU-kenniscentrum voor cyberbeveiliging (ECCC) groen licht gekregen van de Raad. Het kenniscentrum in Boekarest zal investeringen in onderzoek, technologie en industriële ontwikkeling op het gebied van cyberbeveiliging samenbrengen en nauw samenwerken met het ENISA. De Raad heeft tevens conclusies uitgebracht over de opbouw van een gezamenlijke cybereenheid, onder meer in het kader van crisisbeheersing tegen het toenemende aantal ernstige cyberincidenten. Die cybereenheid zou de vorm aannemen van een platform die de gaten in de bestaande samenwerking tussen EU-instanties en nationale autoriteiten moet dichten. Zie ook hier.

Op 29 oktober 2021 zijn regels gepubliceerd die de cyberveiligheid van alle draadloze apparaten die met het internet zijn verbonden, moeten vergroten. Het gaat dan bijvoorbeeld over routers, beveiligings-camera’s, slimme thermostaten, koelkasten, verlichting en deurbellen. Een van de eisen is dat de consument voor ingebruikname van het slimme apparaat eerst zelf een sterk wachtwoord moet instellen in plaats van dat een zwak standaardwachtwoord volstaat. Ook moeten de slimme apparaten regelmatig en gemakkelijk geüpdatet kunnen worden. Producten die medio 2024 niet aan de minimumeisen voldoen, worden verboden.

Europese Cloud

Microsoft gaat investeren in een cloud voor Europese bedrijven en overheden, waarbij alle gegevens worden opgeslagen op servers binnen de Europese grenzen.

In het kader van Project Gaia-X, het door de Franse en de Duitse regering geïnitieerde cloudcomputing-initiatief, zijn onlangs parlementaire vragen gesteld aan de Commissie.

Open Source Software

In opdracht van de Commissie is een studie uitgevoerd naar de impact van open source software en hardware op technologische onafhankelijkheid, concurrentievermogen en innovatie in de EU-economie. Tevens zal de Commissie in navolging van de in 2020 gepresenteerde open source strategie haar software open source toegankelijk maken wanneer er potentiële voordelen zijn voor burgers, bedrijven of overheden.

Nationaal niveau

Verkoop goederen en Levering digitale diensten en digitale inhoud

De verwachte inwerkingtreding van de Implementatiewet Richtlijnen verkoop goederen en levering digitale diensten was 1 januari 2022, maar het wetsvoorstel is nog in behandeling bij de Tweede Kamer. Het wetsvoorstel beoogt de Europese richtlijnen inzake Verkoop van Goederen en Levering Digitale Diensten en Digitale Inhoud te implementeren. Deze Richtlijnen hebben maximum-harmonisatie van het consumentenkooprecht als uitgangspunt. Een belangrijke vernieuwing ten opzichte van het huidige consumentenkooprecht is dat consumenten zowel voor digitale inhoud (bijvoorbeeld games, applicaties), digitale diensten (bijvoorbeeld streaming), als voor goederen met een digitaal element (bijvoorbeeld een smart TV) recht

krijgen op (beveiligings-)updates zolang zij die redelijkerwijs mogen verwachten.

Digitaliseringsstrategie

Op 26 april 2021 heeft staatssecretaris Keijzer een update van de Nederlandse digitaliseringsstrategie aan de Tweede Kamer gestuurd. In deze editie staat een terugblik op drie jaar digitaliseringsbeleid centraal, maar met een blik op de digitale toekomst. Er wordt onder meer melding gemaakt van de instelling van een vaste Kamercommissie Digitale Zaken en de versterking van de samenwerking met coalities als de AI Coalitie, de Alliantie Digitaal Samenleven en de Data Sharing Coalition. Voor het jaar 2021 wordt met name ingezoomd op AI, data, digitale vaardigheden, digitale connectiviteit en digitale weerbaarheid. Tevens is een toekomst-verkenning naar de belangrijkste trends en ontwikkelingen in de digitalisering richting 2030 opgesteld. Gesignaleerde trends zijn onder meer dat kunstmatige intelligentie in de komende jaren steeds vaker zelfstandiger gaat handelen, ook in geval van meer complexere taken en dat steeds meer virtuele werelden zullen worden gecreëerd waardoor vermaak, werk en onderwijs zich naar de virtuele werkelijkheid verplaatsen. Tegelijkertijd wordt in de trends gesignaleerd dat door deze afhankelijkheid van technologische systemen en hun ontwikkelaars, we zowel in handelsconflicten maar ook ten opzichte van cyberspionage, kwetsbaar worden.

Digitale infrastructuur

De ACM heeft de markt IP Interconnectie onderzocht. Daarin kwam naar voren dat Nederland een goede digitale infrastructuur heeft, dat er goed toezicht is en dat er concurrentie is. Wel geeft de ACM aan dat grote partijen steeds vaker direct met elkaar verbinden en dan vaak met gesloten beurs. Kleinere partijen zijn meer aangewezen op zogenaamde internet exchanges, tussenschakels en contracten tegen betaling. De hierboven al genoemde Nederlandse Digitaliseringsstrategie verwijst naar een coronastresstest van het World Economic Forum, waarin naar voren komt dat Nederland (samen met de Scandinavische landen) tot de selecte groep van landen behoort die het beste in staat zijn om zich uit de coronacrisis te transformeren.

Cybersecurity

Op 30 november 2021 heeft minister Blok de Tweede Kamer in een brief geïnformeerd over de voortgang Roadmap Digitaal Veilige Hard- en Software. Deze Roadmap maakt onderdeel uit van de Rijksbrede aanpak voor digitale veiligheid in de Nederlandse Cyber Security Agenda (NCSA) en bestaat uit een combinatie van Europese en nationale maatregelen. De minister wijst in zijn brief aan de Kamer onder andere op de Uitvoeringswet cyberbeveiligings-verordening. Het wetsvoorstel is in behandeling bij de Tweede Kamer. Op basis van deze wet is Agentschap Telecom als toezichthouder aan-gewezen. De minister geeft aan dat de Online Trust Coalitie een witboek heeft gepubliceerd waarin een aantal acties zijn beschreven die bijdragen aan het aantonen van de betrouwbaarheid en veiligheid van clouddiensten. In dat witboek worden drie pijlers gepresenteerd: intrinsieke betrouwbaarheid van clouddiensten op basis van geharmoniseerde standaarden, het bieden van zekerheid door middel van een onafhankelijk verstrekte assurance-verklaring en eenduidige en geharmoniseerde rapportage hierover. Deze pijlers worden meegenomen in de Nederlandse inbreng voor de ontwikkeling van het eerder al genoemde Europese cybersecurity-certificeringsschema voor cloud-diensten. Verder is de risicoklasseindeling beschikbaar op de website van het Digital Trust Center. Deze is bedoeld om voor ondernemers inzichtelijk te maken wat hun risicoprofiel is en welke maatregelen daarbij horen. De minister wijst er tevens op dat op de website van het Centrum voor Criminaliteitspreventie een certificeringsschema is gepubliceerd voor pentesten. Een ander relevant thema in de Kamerbrief is het instrument inkoopeisen Cybersecurity Overheid. Hiermee kunnen opdrachtgevers ten behoeve van IT-inkopen en -aanbestedingen specifieke beveiligingseisen formuleren. Deze eisen kunnen in het contract met de leverancier worden opgenomen. Dit instrument bestaat inmiddels uit tien inkoopsegmenten, waaronder clouddiensten en serverplatforms.

Ransomware

Op 28 juni 2021 heeft minister Grapperhaus een Kamerbrief gepubliceerd over de aanpak van cybercrime. In die brief wordt onder meer de toename van het aantal registraties van computervredebreuk in cijfers weergegeven. Ook geeft de minister aan dat de politie inmiddels met een landelijk dekkende aanpak werkt, bestaande uit onder meer het Team High Tech Crime (THTC) en tien cybercrimeteams in de regionale eenheden. Tevens verwijst de minister naar de omvangrijke internationale politieoperatie Ladybird, dat het complexe netwerk van servers achter de agressieve malware Emotet uit de lucht haalde. De malware besmette de systemen van ruim 1 miljoen slachtoffers wereldwijd. Twee van de drie hoofdservers bleken in Nederland te staan. Ook preventie in de zin van cyberweerbaarheid van burgers, bedrijven en instellingen komt in de Kamerbrief aan bod. In de Kamerbrief wordt tevens gerefereerd aan het Cybersecuritybeeld Nederland 2021 zoals vastgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), welk document hier is te vinden. In een Kamerbrief inzake de Nederlandse Cyber Security Agenda gaat de minister ook inhoudelijk op dit rapport in. Ook heeft minister Grapperhaus naar aanleiding van Kamervragen aangegeven dat wordt onderzocht of het mogelijk is om verzekeraars te

verbieden om betaald losgeld aan cybercriminelen na een ransomware-aanval te vergoeden.

Zerodays

Vorig jaar schreven we over het (gewijzigde) wetsvoorstel Zerodays, dat als doel heeft een wettelijk geborgd afwegingskader te bieden voor alle Zerodays die de overheid ontdekt, aankoopt of anderszins in bezit krijgt. Zerodays zijn fouten in software die nog onbekend zijn bij de maker van de software en die kunnen worden gebruikt om de systemen waarop deze software is geïnstalleerd, te hacken. Op 9 februari 2021 is de stemming over het wetsvoorstel wederom uitgesteld.

Cloudservices

De ACM heeft aangekondigd te onderzoeken of de markt voor Cloudservices goed werkt voor mensen en bedrijven in Nederland. Cloudservices staan op de lijst van core platform services in de concept Digital Markets Act van de Europese Commissie. De ACM geeft aan dat het aldus mogelijk is dat Cloudservices van bedrijven die als poortwachter zijn aangewezen op termijn onder de werking van deze wet vallen.

Nationaal Groeifonds

Het Nationaal Groeifonds is in 2020 gestart. Dit fonds houdt in dat het kabinet voor de periode 2021-2026 twintig miljard euro beschikbaar stelt voor projecten op het gebied van kennisontwikkeling, onderzoek en innovatie en infrastructuur. Er wordt onder meer financiering toegekend aan AiNed (kunstmatige intelligentie), QuantumDeltaNL (quantumtechnologie voor veilige netwerken en communicatie), twee onderwijsprojecten en Health-RI (nationale gezondheidsdata-infrastructuur). Ten behoeve van de verankering van het doel en de werking van het Nationaal Groeifonds en het vastleggen van de criteria voor een bijdrage, is er een Wetsvoorstel Nationaal Groeifonds ingediend bij de Tweede Kamer.

Jurisprudentie

Zorgplicht

Zoals in de inleiding al naar voren kwam, was de zorgplicht het afgelopen jaar minder aanwezig in de gepubliceerde rechtspraak.

Een uitspraak waarin de zorgplicht mede centraal stond, betrof de installatie van een back-up systeem. Volgens de rechtbank Noord-Holland bood een niet nader toegelichte zorgplicht onvoldoende grondslag voor de stelling dat het back-up systeem ook door de IT-leverancier moest worden onderhouden. Ook kon niet van de IT-leverancier worden verwacht dat hij op eigen initiatief het geïnstalleerde back-up systeem aanpaste toen zijn afnemer overstapte op een ander softwareprogramma. Wel moest de IT-leverancier, zodra hij ervan op de hoogte raakte dat de afnemer overstapte op een ander softwareprogramma, de afnemer en/of de nieuwe IT-leverancier erop attenderen dat voor het nieuwe softwareprogramma geen back-upkoppeling bestond.

In een kort geding over de verhuizing van een datacenter werd zijdelings een beroep gedaan op de zorgplicht. De afnemer stelde dat een IT-leverancier de bijzondere plicht heeft, mede vanwege de omvang van de dienstverlening en de afhankelijkheid van de afnemer van het datacenter, om de verwezenlijking van de risico's van een verhuizing te voorkomen. De afnemer eiste daarom onder meer dat er een tastbaar verhuisplan zou komen. De rechtbank ging niet expliciet in op de stelling inzake de zorgplicht, maar overwoog dat de IT-leverancier een zorgvuldige aanpak voorstond, omdat hij een gespecialiseerde senior projectmanager had aangenomen, een stappenplan had gevolgd en een projectteam ten behoeve van de verhuizing had opgericht. Nu er evenmin een contractuele of wettelijke verplichting bestond om een verhuisplan op te stellen, werden de vorderingen van de afnemer afgewezen.

Een IT-leverancier die een koppeling tot stand heeft gebracht met het door zijn afnemer gebruikte boekhoudprogramma werd niet aansprakelijk geacht voor de schade die was ontstaan doordat gegevens uit het boekhoudprogramma werden overschreven bij het gebruik van de koppeling. Het probleem lag niet in de koppeling, maar in de verwerking van de gekoppelde gegevens in het boekhoudprogramma. Het hof Arnhem-Leeuwarden oordeelde dat de afnemer verantwoordelijk is voor zijn eigen boekhouding en dat hij daarvan een back-up had moeten maken om schade te voorkomen. De eventuele schending van een informatie- en waarschuwingsplicht door de IT-leverancier woog hier, mede in verband met de omstandigheden van het geval, onvoldoende zwaar.

Uitleg overeenkomst

Uitspraken waarin de rechters terugvielen op de uitleg van de overeenkomst voor zowel het bestaan van de verplichtingen als de vraag of er sprake was van een tekortkoming, waren er het afgelopen jaar des te meer.

Het hof Arnhem-Leeuwarden kwam aan de hand van een uitgebreide uitleg van de tussen partijen overeengekomen SLA tot de conclusie dat partijen geen concrete norm hadden afgesproken over de mate van beschikbaarheid van de digitale werkomgeving. Daarbij speelde onder meer een rol dat de afnemer voor het laagst mogelijke service level had gekozen. Daaraan deed niet af dat de IT-leverancier in het aanbod had opgenomen dat de systemen een gegarandeerde continuïteit moesten kunnen bieden. Volgens het hof betrof dit duidelijk

wervende teksten. Een professionele partij mag daaraan niet zomaar de verwachting verbinden dat zij - op basis van wat er uiteindelijk in de SLA is overeengekomen - een nagenoeg storingsvrije toegang zou hebben.

De voorzieningenrechter te Overijssel oordeelde dat in kort geding niet kon worden vastgesteld wat partijen onderling exact hebben afgesproken inzake de facturering omdat slechts sprake was van een mondelinge overeenkomst. Wel was de voorzieningenrechter van mening dat vanwege de afhankelijkheid van de diensten van de IT-leverancier, deze de dienstverlening (voorlopig) diende voort te zetten. De IT-leverancier moest daarvoor wel een redelijke vergoeding ontvangen. De door de IT-leverancier voldoende onderbouwde maandelijkse vergoeding werd door de afnemer onvoldoende weersproken en kwam de voorzieningenrechter mede gelet op de facturatiegeschiedenis, niet onredelijk voor.

Ook in een geschil over het al dan niet functioneren van printplaten was onduidelijk wat partijen waren overeengekomen. Alvorens tot uitleg van de overeenkomsten over te gaan, zag het hof Den Bosch echter aanleiding om een deskundige te benoemen teneinde te kunnen beoordelen of de printplaten functioneren. Het hof gaf wel alvast een voorzet inzake de omstandigheden die het relevant acht voor de uitleg van de overeenkomsten, namelijk dat sprake is van twee professionele partijen, dat het een redesign overeenkomst (doorontwikkeling bestaand product) betreft en ook dat de tekst van de overeenkomst is opgesteld door de IT-leverancier. Wat het hof daar vervolgens mee zal doen, is dus nog even afwachten.

Het hof Arnhem-Leeuwarden oordeelde dat de IT-leverancier een overeenkomst tot het bouwen van een funnel was nagekomen. Uit de verschillende overeenkomsten kon niet worden vastgesteld dat de IT-leverancier de door de opdrachtgever gestelde werkzaamheden diende uit te voeren.

In een geschil over de oplevering van een hydraulieksysteem kwam de rechtbank te Overijssel tot het oordeel dat partijen geen specifieke en duidelijke afspraken hadden gemaakt over de specificaties van de software.

In een kort geding over de ontvlechting van een samenwerkingsovereenkomst stelde de IT-leverancier dat de contractuele nazorgverplichting niet gold omdat deze was opgenomen in het artikel met de kop ‘ontbinding’, terwijl de overeenkomst was geëindigd doordat de looptijd was verstreken. Het hof Amsterdam legde de bepaling mede uit in het licht van eerdere overeenkomsten tussen partijen. Die overeenkomsten hadden op bepaalde punten hun gelding behouden omdat zij op elkaar voortbouwden en in de laatste overeenkomst werd terugverwezen naar die eerdere overeenkomsten. Uit die overeenkomsten, gelezen in samenhang met de laatste overeenkomst, volgde dat de nazorgverplichting gold voor alle gevallen waarin de overeenkomst eindigde. Een andere uitleg zou ook tot het merkwaardige resultaat leiden dat op de IT-leverancier wél een nazorgverplichting zou gelden in het geval van een tekortschietende wederpartij, maar niet als de overeenkomst eindigt zonder dat de wederpartij is tekortgeschoten, aldus het hof.

De rechtbank Rotterdam oordeelde dat er ondanks dat niet voldaan was aan het schriftelijkheidsvereiste in de intentieverklaring, een overeenkomst tussen partijen tot stand was gekomen. Partijen hadden uitvoering gegeven aan de gemaakte maar niet ondertekende overeenkomst en waren het ook met elkaar eens over die afspraken. Partijen zijn daardoor stilzwijgend voorbijgegaan aan de schriftelijkheidseis.

De rechtbank Amsterdam vulde de beëindigings-overeenkomst die tussen partijen was gesloten aan voor wat betreft de financiële afrekening, omdat partijen daarover geen overeenstemming hadden bereikt. De rechtbank sloot in dit kader aan bij artikel 7:411 BW inzake een redelijk loon. De omstandigheden die meewogen waren de al verrichte werkzaamheden en het voordeel dat de opdrachtgever daarvan heeft. De rechtbank overwoog dat dit voordeel slechts beperkt was. De uitkomst was dat de opdrachtgever in ieder geval de waarde diende te vergoeden die de werkzaamheden volgens zijn eigen stellingen vertegenwoordigde en daarnaast een derde van het bedrag dat daarna nog overbleef.

De opzegtermijn van een overeenkomst op basis waarvan een IT-consultant zou worden gedetacheerd bij derden, is door het hof Amsterdam bepaald door middel van een redelijke uitleg van die overeenkomst in het licht van de overige bepalingen van de overeenkomst en toepassing van artikel 7:411 BW (inzake een redelijk loon bij beëdiging van de opdracht).

Inspanningsverbintenis

De rechtbank Amsterdam overwoog dat een “gewenste uitkomst” tot het behalen van zes nieuwe klanten in 2019, geen resultaatsverbintenis betreft. Volgens de afnemer was dit wel het geval vanwege de bepaling in de algemene voorwaarden dat “*de Overeenkomst het karakter draagt van een inspanningsverbintenis, tenzij en voorzover in de schriftelijke Overeenkomst uitdrukkelijk een resultaat is toegezegd en het betreffende resultaat tevens met voldoende bepaaldheid is omschreven in de Overeenkomst*”. De rechtbank ging daar dus niet in mee. Verder gaf de rechtbank aan dat het al dan niet voldoen aan een resultaatsverbintenis of

inspanningsverbintenis niet zonder meer betekent dat eiseres van haar betalingsverplichting zou worden bevrijd.

Back-ups

Ook dit jaar waren er weer verschillende uitspraken waarin het belang van en de verantwoordelijkheid voor back-ups centraal stond in geval van een ransomware-aanval. Enkele hiervan kwamen al aan de orde in het kader van de zorgplicht. Daar zagen we al dat de verantwoordelijkheid voor back-ups niet altijd alleen bij de IT-leverancier werd gelegd.

Ten aanzien van een hack die plaatsvond nadat de SLA met de IT-leverancier was geëindigd, maar voordat de SLA met de nieuwe IT-leverancier was ingegaan, verdeelde het hof Amsterdam de aansprakelijkheid voor de schade tussen de IT-leverancier en zijn ex-afnemer. Het hof oordeelde dat op de einddatum van de SLA een recente volledige back-up aanwezig had moeten zijn, althans dat deze had moeten kunnen worden gereconstrueerd. De afnemer zou echter ook schade hebben geleden als er wel een volledige back-up aanwezig was geweest op de einddatum van de SLA, omdat de hack “in between SLA’s” plaatsvond. Om die reden liet het hof 2/3 van de door de afnemer geleden schade voor rekening van de afnemer zelf komen.

Onder de verantwoordelijkheid voor de "24/7 monitoring van servers, back-ups en netwerk" vielen volgens de rechtbank Rotterdam tevens de bestanden met daarop door een derde partij ontwikkelde maatwerksoftware. Ten behoeve van de back-up van die bestanden was er een aparte map (SQLBackup) aangemaakt. De IT-leverancier nam deze map mee in de dagelijkse back-up, maar na een ransomware-aanval bleek dat de bestanden met maatwerksoftware verloren waren gegaan. De IT-leverancier stelde onder meer dat dit kwam omdat de derde partij de nieuwe, gewijzigde bestanden niet had weggeschreven naar de SQL back-up map. De rechtbank heeft een deskundigenbericht gelast, onder andere vanwege de vraag of de IT-leverancier ervan uit mocht gaan dat de SQL back-up map door de derde partij werd gevuld.

Wat afwijkend is de uitspraak van de kantonrechter te Rotterdam. De kantonrechter oordeelde dat de verantwoordelijkheid van de webhoster voor de bereikbaarheid van de website van eiseres, tevens inhoudt het voorkomen van blootstelling aan door derden veroorzaakte digitale inbreuken op die bereikbaarheid.

Klachtplicht

Geen IT-geschil, maar relevant voor de IT-praktijk is dat de Hoge Raad heeft geoordeeld dat artikel 6:89 BW inzake de klachtplicht niet van toepassing is wanneer de prestatie in het geheel niet is verricht. Degene die een prestatie heeft verricht moet erop kunnen rekenen dat de schuldeiser met bekwame spoed onderzoekt of de prestatie aan de verbintenis beantwoordt en indien dat niet het geval is, dit met bekwame spoed aan hem meedeelt. De strekking van artikel 6:89 BW verzet zich dus tegen toepassing indien de prestatie niet is verricht. Interessant was dat eiser in feitelijke instanties niet had gesteld dat artikel 6:89 BW niet van toepassing was. Het hof was ambtshalve gehouden de juiste rechtsregel toe te passen (art. 25 Rv) aldus de lezenswaardige conclusie van de P-G.

Een afnemer die intensief bij de werkzaamheden betrokken is geweest en daarover een zekere mate van controle had, had kunnen en moeten ingrijpen indien hij van mening was dat de IT-leverancier niet aan zijn verplichtingen voldeed of buiten de opdracht werkte (te veel uren declareerde). De rechtbank Noord-Holland woog tevens mee dat het een project op basis van nacalculatie was en dat de afnemer als *'product owner*' verantwoordelijk was voor de progressie, scope en kosten. Interessant is dat de rechtbank een belangrijke rol toedicht aan de appconversaties tussen afnemer en IT-leverancier. Deze speelden een rol bij de vraag of de afnemer in gebreke is gesteld en ook bij de vraag of de afnemer al dan niet heeft ingestemd met bepaalde werkzaamheden.

Verzuim

Een fatale termijn kan volgens het hof Amsterdam ook een bepaalde periode beslaan. Het hof oordeelde dat het in overleg verplaatsen van een deadline die een fatale termijn was, hieraan niet het fatale karakter ontnam, maar dat dit “de fatale termijn slechts heeft verlengd”. Het fatale karakter van de termijn bleek volgens het hof uit de stukken en verklaringen ter zitting, omdat daaruit volgde dat de software per 1 januari 2018 live zou gaan. Gelet daarop had de IT-leverancier zijn betoog, dat hij door het verstrijken van die datum niet in verzuim is geraakt, nader moeten toelichten. Het verschuiven van de termijn (“doormodderen”) had in deze zaak dus geen consequenties voor de afnemer.

De rechtbank Rotterdam vond dat een afnemer niet voldoende concreet had uitgelegd waarom een lijst van onvolkomenheden en next steps, zonder het gunnen van een laatste termijn voor nakoming, zou maken dat van de afnemer niet kon worden gevergd dat hij doorging met het project en de overeenkomst zonder ingebrekestelling mocht ontbinden.

De Hoge Raad heeft geoordeeld dat de cassatieklachten van Alert tegen de arresten van het hof Den Bosch van 3 november 2015 en 17 december 2019 niet kunnen leiden tot vernietiging van die arresten. Procureur-Generaal Wissink concludeerde eveneens tot verwerping van het cassatieberoep. De P-G gaat in op de cassatieklachten van Alert inzake de aard van de

termijnen en of overschrijding ervan schending van een material obligation kan opleveren. Ook de overwegingen inzake anticipatory breach zijn interessant.

Ontbinding

Een IT-leverancier mocht de overeenkomst inzake de ontwikkeling van drie websites ontbinden omdat de afnemer geen content aanleverde ten behoeve van de websites. Het verweer van de afnemer dat er geen overeenkomst tot stand is gekomen onder andere omdat er geen getekende offerte is, hield geen stand. De kantonrechter te Noord-Holland leidde het bestaan van de overeenkomst af uit de gedragingen en verklaringen van partijen. Onweersproken was dat negentig procent van de overeengekomen werkzaamheden reeds was verricht. De afnemer werd dan ook veroordeeld tot betaling van die werkzaamheden (waardevergoeding in het kader van ongedaanmakingsverplichtingen).

Schade

De rechtbank Overijssel oordeelde dat het uitsluitend ter beschikking willen stellen van een team van vijf consultants, terwijl de afnemer slechts verplicht was om één consultant af te nemen, een voldoende ernstige tekortkoming betreft om ontbinding van de overeenkomst te rechtvaardigen. De rechtbank kon de afnemer echter niet volgen in het standpunt dat deze naast terugbetaling van betaalde facturen (minus een waardevergoeding voor niet ongedaan te maken prestaties), schade had geleden. De schade zou zijn gelegen in het verlies van manuren, winstderving en advocaatkosten, maar met die summiere stellingen heeft de afnemer niet aan zijn stelplicht voldaan, hoe beperkt die voor een verwijzing naar de schadestaatprocedure ook is.

De rechtbank Overijssel wees op het belang van het onderbouwen van het causaal verband tussen de fouten in de software en de gestelde schade. Dit was in dit geschil met name relevant omdat de voortgang van het project (tevens) te lijden had gehad onder diverse andere problemen.

Opzegging

De opzegging van een samenwerking door een reseller, waarna deze een eigen, zelfde soort softwaretool aan gezamenlijke klanten aanbood, kwam hem duur te staan. Het betrof een Information Security Management System die door de reseller aan verschillende gemeenten was verkocht, waarbij contracten voor bepaalde tijd waren gesloten. Op enig moment heeft de reseller de samenwerking met de IT-leverancier opgezegd en de door hem zelf ontwikkelde ISMS-tool aan de gemeenten aangeboden. Verschillende gemeenten kozen voor de tool van de reseller. De IT-leverancier stelde zich op het standpunt dat de reseller de betalingsverplichtingen jegens de IT-leverancier uit hoofde van de contracten voor bepaalde tijd met de gemeenten diende na te komen. De rechtbank gaf de IT-leverancier gelijk voor wat betreft de betalingsverplichtingen uit hoofde van reeds aangevangen contractjaren. Dat de gemeenten zelf voor de ISMS-tool van de reseller hadden gekozen en dat op grond van de algemene voorwaarden van de reseller ook mochten, kon daaraan niet in de weg staan. De reseller had de gemeenten om hem moverende redenen onverplicht een keuze-mogelijkheid geboden, wat voor zijn eigen rekening en risico behoorde te blijven.

Softwareauteursrecht - contractenrecht

Het hof Amsterdam oordeelde in een kort geding dat geen van beide partijen haar uitleg van de exclusiviteitsbepaling inzake de ontwikkeling van software voor een medisch instrument aannemelijk heeft kunnen maken. Het was echter aan eiseres, die stelde dat gedaagde inbreuk maakt op de exclusiviteitsbepaling, om aannemelijk te maken dat zij aanspraak kan maken op de exclusiviteit. Nu eiseres daarin niet is geslaagd, zijn de vorderingen van eiseres (alsnog) afgewezen.

Volgens het Hof van Justitie valt onder artikel 4 van de richtlijn betreffende de rechtsbescherming van computerprogramma's ook het decompileren van software onder de voorbehouden handelingen van de rechthebbende van een computerprogramma. Het hof is echter van oordeel dat decompilatie ook toegestaan kan zijn onder de algemene uitzondering op de voorbehouden handelingen van artikel 5 van de richtlijn. De software mag ook worden gedecompileerd om fouten te verbeteren die de werking van de software beïnvloeden. Dit is echter alleen toegestaan als die decompilatie noodzakelijk is voor het verhelpen van die fouten en in voorkomend geval met inachtneming van de tussen partijen gesloten overeenkomst. Het hof volgt daarmee de conclusie van de AG.

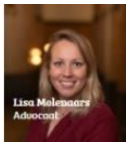
Meer weten?

Neem dan contact op met een van onze specialisten:

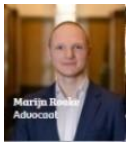
Huub de Jong

Annemarie Bolscher

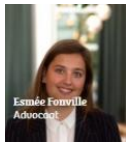
Tom de Wit



Lisa Molenaars



Marijn Rooke



Esmee Fonville